UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Megan Murillo, on behalf of herself individually and on behalf of all others similarly situated, Plaintiff, v. Pawn America Minnesota, LLC; Payday America, Inc.; and PAL Card Minnesota, LLC., Defendants.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Megan Murillo ("Plaintiff"), on behalf of herself and all others similarly situated (the "Class Members"), brings this Class Action Complaint against Defendants Pawn America Minnesota, LLC; Payday America, Inc.; and PAL Card Minnesota, LLC (collectively "Pawn America" or "Defendants"). The allegations in this Complaint are based on the personal knowledge of Plaintiff or upon information and belief and investigation of counsel.

NATURE OF CASE

1. This is a data breach class action brought on behalf of consumers whose sensitive personal information was stolen by cybercriminals in a massive cyber-attack at Pawn America in or around September 2021 (the "Data Breach"). The Data Breach reportedly involved collectively at least 530,000 consumers of Defendants.

2. Information stolen in the Data Breach included individuals' sensitive information, including Full names; Social Security numbers; Driver's license numbers; Passport numbers; Government identification numbers; Dates of birth; and Financial account information (collectively the "Private Information" or "PII").

3. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of loss of the value of their private and confidential information, loss of the benefit of their contractual bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

4. Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendants, their officials, and agents—was compromised, unlawfully accessed, and stolen due to the Data Breach.

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Plaintiff's and Class Members' Private Information that it collected and maintained.

6. Defendants maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendants' computer network in a condition vulnerable to cyberattacks of this type.

7. Upon information and belief, the mechanism of the cyber-attack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known and foreseeable risk to Defendants, and Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. In addition, Defendants and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendants properly monitored their property, they would have discovered the intrusion sooner.

9. Because of the Data Breach, Plaintiff and Class Members suffered injury and damages in the form of theft and misuse of their Private Information.

10. In addition, Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct since the Private Information that Defendants collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the cyber-attack, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. As a further result of the Data Breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiff and Class Members have and may also incur out-of-pocket costs, e.g., for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of: the loss of time needed to: take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits, charges, and fees charged against their accounts; and deal with spam messages and e-mails received as a result of the Data Breach. Plaintiffs and Class Members have likewise suffered and will continue to suffer an invasion of their property interest in their own Private Information such that they are entitled to damages for unauthorized access to and misuse of their Private Information from Defendants. And, Plaintiff and Class Members presently and will continue to suffer from damages associated with the unauthorized use and misuse of their Private Information as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

15. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or removed from the network during the Data Breach.

16. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring and identity restoration services funded by Defendants.

17. Accordingly, Plaintiff brings this action against Defendants seeking to redress their unlawful conduct.

PARTIES

18. Plaintiff Megan Murillo is a resident and citizen of the city of Artesia in the State of New Mexico. Plaintiff Murillo is acting on her own behalf and on behalf of others similarly situated. Ms. Murillo received a Notice of the Data Breach from Defendants in or around November 2021. The Notice advised her that the Data Breach had occurred and that her Private Information was accessed and compromised. Defendants obtained and continue to maintain Plaintiff Murillo's Private Information and have a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Murillo would not have entrusted her Private Information to Defendants had she known that Defendants would fail to maintain adequate data security. Plaintiff Murillo's Private Information was compromised and disclosed as a result of the Data Breach.

19. Defendant Pawn America Minnesota LLC is a limited liability company formed under the laws of the State of Minnesota, with its principal place of business at 181 River Ridge Circle South in the City of Burnsville, County of Dakota, State of Minnesota.

20. Defendant Payday Minnesota, Inc. is a corporation formed under the laws of the State of Minnesota, with its principal place of business at 181 River Ridge Circle South in the City of Burnsville, County of Dakota, State of Minnesota.

21. Defendant PAL Card Minnesota, LLC is a limited liability company formed under the laws of the State of Minnesota, with its principal place of business at 181 River Ridge Circle South in the City of Burnsville, County of Dakota, State of Minnesota.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

23. This Court has personal jurisdiction over Defendants as Defendants' principal places of business are located within this District.

24. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District; Defendants reside within this judicial district; and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

FACTUAL ALLEGATIONS

Background

25. Defendants own and operate payday lending stores and pawnshops throughout the States of Minnesota and Wisconsin.

26. According to its website, Defendant Pawn America Minnesota, LLC operates 17 pawn shops in Minnesota and Wisconsin, having been founded approximately thirty years ago.[1]

27. Defendant Payday America, Inc. "has been providing guests with short-term banking options for more than a decade. [It] currently operate[s] 12 stores throughout Minnesota."[2]

28. Defendant PAL Card Minnesota, LLC operates under the trade name of CashPass marketing, distributing, and supporting prepaid payment cards.

29. In the ordinary course of doing business with Defendants, customers, like Plaintiff, and prospective customers are required to provide Defendants with sensitive PII such as:

a. Full names;

b. Social Security numbers;

c. Driver's license numbers;

d. Passport numbers;

e. Government identification numbers;

f. Dates of birth; and

g. Financial account information.

30. As a condition of transacting with Defendants, Plaintiff and Class Members were required to disclose some or all of the Private Information listed above.

[1] https://www.pawnamerica.com/about-pawn-america (last visited Nov. 29, 2021).
[2] https://www.paydayamerica.com/about-us/ (last visited Nov. 29, 2021).

31. On information and belief, in the course of collecting Private Information from consumers, including Plaintiff, Defendants promised to provide confidentiality and adequate security for customer data through their applicable privacy policy and through other disclosures.

32. Defendant Pawn America Minnesota LLC, provides a privacy policy on its website, speaking for the other Defendants as part of the "Rixmann Companies," wherein it states that "we take the protection of your personal information very seriously."[3]

33. Defendant PAL Card Minnesota, LLC provides for its customers a similar privacy policy.[4]

34. Defendant Payday America, Inc., in its privacy policy, informs its customers that it is "committed to the security and confidentiality of your non-public personal information. Our security practices include limiting access to this information to those employees and business associates with appropriate authority and for intended business purposes only."[5]

35. Defendant Payday America Inc. promises that "[t] o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[6]

---

[3] https://www.pawnamerica.com/privacy-policy (last visited Nov. 29, 2021).
[4] *See* privacy policy link at https://www.cashpass.com/disclosures/ (last visited Nov. 29, 2021).
[5] *See* privacy policy link at https://www.paydayamerica.com/about-us/ (last visited Nov. 29, 2021).
[6] *Id.*

The Data Breach

36. On or about September 28, 2021, Defendants began experiencing outages and thereafter discovered that they had permitted a ransomware attack to occur on their computer network and systems.

37. Defendants claim that they discovered the Breach was on October 3, 2021.[7]

38. However, despite first learning of the Data Breach on or about October 3, 2021, Defendants did not take any "measures" to notify affected Class Members until at least October 25, 2021, with affected Class Members not being sent notice until November 2021.

39. Defendants admit that Plaintiff's and Class Members' Private Information was "compromised" in the Data Breach. In fact, Defendants informed Plaintiff and members of the Class in their Notice of Data Breach that "[t]he cybercriminal…retained copies of much of the data and threatened to leak the information which could make it available to other cybercriminals."

40. On information and belief, Defendants failed to encrypt the PII stored on their systems, evidenced by the fact that hackers were able to steal the Private Information in a readable form.

41. Defendants acknowledge their cybersecurity and data protection was inadequate because they admit that, following the Data Breach, they are working to "improve [their] security."

[7] *Supra*, n.3.

42. Defendants also acknowledges that Plaintiff and Class Members face a substantial and present risk of identity theft because they are actively encouraging them to take steps to "protect your information," including "how to place a fraud alert or a security freeze on your credit file."

43. Based on the Notice of Data Breach letter she received, which informed Plaintiff that her Private Information was removed from Defendants' network and computer systems, Plaintiff believes her Private Information was stolen from Defendants' network and systems (and subsequently sold) as a result of the Data Breach.

44. Further, the removal of the Private Information from Defendants' system demonstrates that this cyberattack was targeted.

45. Additionally, though Plaintiff and Class members have an interest in ensuring that their information remains protected, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures taken to ensure a breach does not occur again have not been shared with regulators, Plaintiff, or Class Members.

46. While Defendants' respective websites bear a link to a notice of the Data Breach dated October 25, 2021, a Class member, if any, who may have seen this notice, but who did not receive any notice of Data Breach from Defendants, would likely conclude that their data was not impacted in the Data Breach and, therefore, would not have known of the need to take action to protect themselves.

47. Defendants have not offered any identity theft monitoring services or assistance, other than the contact information for the Federal Trade Commission, and a link to the website of the Federal Trade Commission ("FTC").[8]

Defendants Were Aware of the Data Breach Risks

48. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

49. Plaintiff and Class Members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to employ reasonable care to keep such information confidential and secure from unauthorized access.

50. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the banking/credit/financial services industry preceding the date of the Data Breach.

51. Indeed, data breaches, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants' industry, including Defendants.

[8] https://www.identitytheft.gov/#/ (last visited Nov 29, 2021).

52. According to the FTC, identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[9] Identity thieves use the stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[10]

53. The PII of Plaintiff and Class Members was taken by cyber criminals for the very purpose of engaging in identity theft, or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

54. Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, driver's license numbers and/or state identification numbers, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result of a breach.

---

[9] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf (last visited Nov. 29, 2021).

[10] *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

55. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. They are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

56. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Defendants Failed to Comply with FTC Guidelines

57. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

58. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

59. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex

passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

60. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

61. Defendants failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

62. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered;

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;

d. Configure firewalls to block access to known malicious IP addresses;

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system;

f. Set anti-virus and anti-malware programs to conduct regular scans automatically;

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary;

h. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares;

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used;

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;

m. Execute operating system environments or specific programs in a virtualized environment; and

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

63. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

1. **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.

2. **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

3. **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

4. **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it.

5. **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

6. **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA

product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

7. **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[11]

64. Defendants were at all times fully aware of their obligation to protect the PII of customers, prospective customers, and employees. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failed to Comply with Industry Standards

65. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendants' cybersecurity practices. Best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

66. Defendant Payday America, Inc.'s privacy policy expresses a compliance with federal law required for "financial companies," as well as "limiting access to this information to those employees and business associates with appropriate authority and for intended business purposes only." This policy refers to the remaining Defendants as "financial companies" as well, and states that federal law applies to the protection and

[11] https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Nov. 29, 2021).

sharing of information. The other Defendants' privacy policies do not make such disclosures as "financial companies."

67. Upon information and belief, Defendants failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendants' industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

68. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach.

Defendants' Breach

69. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems, networks, and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor their data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords, and;

i. Failing to properly train and supervise employees in the proper handling of inbound emails.

70. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

71. Accordingly, as outlined below, Plaintiffs and Class Members now face a substantial, increased, and present risk of fraud and identity theft.

72. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft.

73. Defendants were well aware that the Private Information it collects is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the operators who perpetrated this cyber-attack.

74. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[12]

75. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

76. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

77. For example, armed with just a name and date of birth, a data thief can use a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social

[12] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Nov. 29, 2021) ("GAO Report").

Security number.

78. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

79. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[13]

80. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

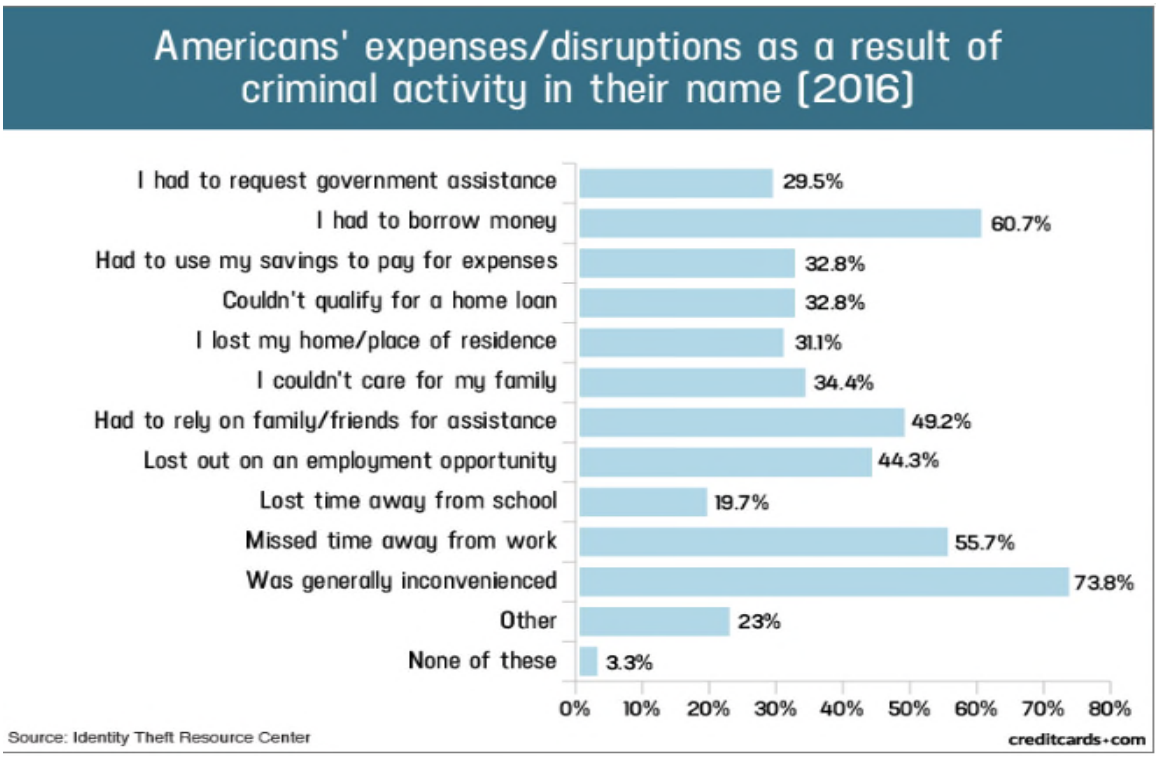
81. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

82. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may

[13] *See* https://www.identitytheft.gov/Steps (last accessed Sept 22, 2021).

even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

83. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[14]



84. What's more, theft of Private Information is also gravely serious. PII is a valuable property right.[15]

---

[14] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020), available at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Nov. 29, 2021).

[15] *See, e.g.*, John T. Soma, *et al.*, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

85. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

86. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

87. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at 29.

88. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

89. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at a substantial and immediate present risk of fraud and identity theft that will continue for many years.

90. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

91. Sensitive Private Information can sell for as much as $363 according to the Infosec Institute.

92. PII is particularly valuable because criminals can use it to target victims with frauds and scams.

93. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

94. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.

95. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

96. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.

97. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

98. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

99. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[16]

100. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[17]

---

[16] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Nov. 29, 2021).

[17] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, available at: http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Nov. 29, 2021).

101. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[18]

102. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

103. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[19] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID

[18] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last visited Nov. 29, 2021).

[19] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited Nov. 29, 2021).

> verification, or use the information to craft curated social engineering phishing attacks."[20]

104. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[21]

105. At all relevant times, Defendants knew or reasonably should have known these risks, the importance of safeguarding Private Information, and the foreseeable consequences if its data security systems were breached, and strengthened their data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

106. Defendants entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

107. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

108. Plaintiff and Class Members presently face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

109. Plaintiff and Class Members have been, and currently face substantial risk of being targeted now and in the future, subjected to phishing, data intrusion, and other

---

[20] *Id.*

[21] *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited Nov. 29, 2021).

illegality based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

110. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

111. Plaintiff and Class members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

112. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

113. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach

114. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

115. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII —which contains the most intimate details

about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

116. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Plaintiff Megan Murillo's Experience

117. Plaintiff Murillo has made in person transactions with one or more Defendant.

118. In making these transactions, Plaintiff Murillo entrusted her PII and other confidential information to Defendants with the reasonable expectation and understanding that Defendants would take, at a minimum, industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff Murillo would not have used Defendants' services had she known that Defendants would not take reasonable steps to safeguard her sensitive PII.

119. Plaintiff Murillo has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This is time that has been lost forever and cannot be recaptured.

120. Plaintiff Murillo stores all documents containing her PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the few online accounts that she has.

121. Plaintiff Murillo has suffered actual injury in the form of damages to, and diminution in, the value of her PII – a form of intangible property that Plaintiff Murillo entrusted to Defendants. This PII was compromised in, and has been diminished as a result of, the Data Breach.

122. Plaintiff Murillo has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

123. Plaintiff Murillo has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII resulting from the compromise of her PII, especially her Social Security number, in combination with her name, address, phone number, and email address, which PII is now in the hands of cyber criminals and other unauthorized third parties.

124. Knowing that thieves stole her PII, including her Social Security number and/or driver's license number and other PII that she was required to provide to Defendants, and knowing that her PII will likely be sold on the dark web, has caused Plaintiff Murillo great anxiety.

125. Plaintiff Murillo has a continuing interest in ensuring that her PII that, upon information and belief, remains in the possession of Defendants, is protected and safeguarded from future data breaches.

126. As a result of the Data Breach, Plaintiff Murillo is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

CLASS ALLEGATIONS

127. Plaintiff brings this nationwide class action pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4), individually and on behalf of all members of the Class:

> All natural persons residing in the United States whose PII was compromised in the Data Breach initially discovered by Defendants on or about October 3, 2021 (the "Class").

128. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

129. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

130. **Numerosity**. The Class is so numerous that joinder of all members is impracticable. The Class includes hundreds of thousands of individuals whose personal

data was compromised by the Data Breach. The exact number of Class Members is in the possession and control of Defendants and will be ascertainable through discovery.

131. **Commonality.** There are numerous questions of law and fact common to Plaintiff and the Class that predominate over any questions that may affect only individual Class Members, including, without limitation:

a. Whether Defendants unlawfully maintained, lost or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their PII;

f. Whether Defendants breached duties to Class Members to safeguard their PII;

g. Whether cyber criminals obtained Class Members' PII in the Data Breach;

h. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Defendants owed a duty to provide Plaintiff and Class Members notice of this Data Breach, and whether Defendants breached that duty to provide timely notice;

j. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

k. Whether Defendants' conduct was negligent;

l. Whether Defendants' conduct violated federal law;

m. Whether Defendants' conduct violated state law; and

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

132. Typicality. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class Members, had her personal data compromised, breached, and stolen in the Data Breach. Plaintiff and all Class Members were injured through the uniform misconduct of Defendants, described throughout this Complaint, and assert the same claims for relief.

133. Adequacy. Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff retained counsel who are experienced in Class action and complex litigation. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other Class Members.

134. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Defendants' wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

135. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendants to have to choose between differing means of upgrading their data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

136. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

137. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Plaintiff and Class Members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

FIRST CLAIM
Negligence
(On Behalf of Plaintiff and the Class)

138. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 137.

139. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

140. The legal duties owed by Defendants to Plaintiff and Class Members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Class Members in Defendants' possession;

b. To protect the PII of Plaintiff and Class Members in Defendants' possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the Data Breach.

141. Defendants' duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendants of failing to use reasonable measures to protect PII.

142. Various FTC publications and data security breach orders further form the basis of Defendants' duty. Plaintiff and Class Members are consumers under the FTC Act. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

143. Defendants breached their duties to Plaintiff and Class Members. Defendants knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

144. Defendants knew or should have known that their security practices did not adequately safeguard the PII of Plaintiff and Class Members.

145. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect the PII of Plaintiff and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendants unlawfully breached their duty to use

reasonable care to adequately protect and secure the PII of Plaintiff and Class Members during the period it was within Defendants' possession and control.

146. Defendants breached the duties they owe to Plaintiff and Class Members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that their systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to Plaintiffs and Class Members that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

147. Due to Defendants' conduct, Plaintiff and Class Members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used for identity theft and other types of financial fraud against them immediately and for years to come.

148. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219.00 to $358.00 per year.

149. As a result of Defendants' negligence, Plaintiff and Class Members suffered injuries that may include:

(i) actual identity theft;

(ii) the lost or diminished value of PII;

(iii) the compromise, publication, and/or theft of PII;

(iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

(v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;

(vi) the continued risk to their PII, which may remain for sale on the dark web and is in Defendants' possession and subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession;

(vii) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members, including ongoing credit monitoring.

150. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and Class Members suffered was the direct and proximate result of Defendants' negligent conduct.

SECOND CLAIM
Negligence Per Se
(On Behalf of Plaintiff and the Class)

151. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 150.

152. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The

FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

153. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendants' magnitude, including, specifically, the immense damages that would result to Plaintiff and Class Members due to the valuable nature of the PII at issue in this case—including Social Security numbers.

154. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

155. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

156. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

157. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

i. actual identity theft;

ii. the lost or diminished value of PII;

iii. the compromise, publication, and/or theft of PII;

iv. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

v. lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;

vi. the continued risk to their PII, which may remain for sale on the dark web and is in Defendants' possession and subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession;

vii. future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members, including ongoing credit monitoring.

158. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and members of the Classes have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

THIRD CLAIM
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

159. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 158.

160. When Plaintiff and Class Members provided their PII to Defendants in exchange for Defendants' products and services, they entered into implied contracts with

Defendants under which—and by mutual assent of the parties—Defendants agreed to take reasonable steps to protect their PII.

161. Defendants solicited and invited Plaintiff and Class Members to provide their PII as part of Defendants' regular business practices and as essential to the sales and employment transactions entered into between Defendants on the one hand and Plaintiff and Class Members on the other. This conduct thus created implied contracts between Plaintiff and Class Members on the one hand, and Defendants on the other hand. Plaintiff and Class Members accepted Defendants' offers by providing their PII to Defendants in connection with their purchases from and employment with Defendants.

162. When entering into these implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws, regulations, and industry standards.

163. Defendants' implied promise to safeguard Plaintiff and Class Members' PII is evidenced by a duty to protect and safeguard PII that Defendants required Plaintiff and Class Members to provide as a condition of entering into consumer transactions and employment relationships with Defendants.

164. Plaintiff and Class Members paid money to Defendants to purchase products or services from. Plaintiff and Class Members reasonably believed and expected that Defendants would use part of the funds received as a result of the purchases or services provided to obtain adequate data security. Defendants failed to do so.

165. Plaintiff and Class Members, on the one hand, and Defendants, on the other hand, mutually intended—as inferred from the continued use of Defendants' services—

that Defendants would adequately safeguard PII. Defendants failed to honor the parties' understanding of these contracts, causing injury to Plaintiff and Class Members.

166. Plaintiff and Class Members value data security and would not have provided their PII to Defendants in the absence of Defendants' implied promise to keep the PII reasonably secure.

167. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendants.

168. Defendants breached their implied contracts with Plaintiff and Class Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

169. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

FOURTH CLAIM
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

170. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 169.

171. Plaintiff brings this cause of action solely in the alternative to her breach of contract claim plead in Count III.

172. Defendants benefited from receiving Plaintiff's and Class members' PII by their ability to retain and use that information for their own benefit. Defendants understood this benefit.

173. Defendants also understood and appreciated that Plaintiff and Class Members' PII was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

174. Plaintiff and Class Members who were customers of Defendants conferred a monetary benefit upon Defendants in the form of monies paid for services from Defendants.

175. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Defendants also benefited from the receipt of Plaintiff and Class Members' PII, as Defendants used it to facilitate the transfer of information and payments between the parties.

176. The monies that Plaintiff and Class Members paid to Defendants for products and services were to be used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

177. Defendants also understood and appreciated that Plaintiff and Class Members' PII was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

178. But for Defendants' willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and untrusted with Defendants. Indeed, if Defendants had informed Plaintiff and Class Members that their data and cyber security measures were inadequate, Defendants would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

179. As a result of Defendants' wrongful conduct, Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members. Defendants continue to benefit and profit from their retention and use of the PII while its value to Plaintiff and Class Members has been diminished.

180. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including compiling, using, and retaining Plaintiff and Class Members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

181. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the amount Plaintiff and Class Members paid for their purchases with reasonable data privacy and security practices and procedures and the purchases they actually received with unreasonable data privacy and security practices and procedures.

182. Under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

183. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds they received as a result of the conduct alleged herein.

FIFTH CLAIM
Violation of the Uniform Deceptive Trade Practices Act
(Minn. Stat. § 325D.44)
(On Behalf of Plaintiff and the Class)

184. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 184 above as if fully set forth herein.

185. The Minnesota Deceptive Trade Practices Act makes unlawful acts performed "in the course of business, vocation, or occupation" that: (a) represent that goods or services have characteristics, uses, or benefits that they do not have; and (b) constitute "any other conduct which similarly creates a likelihood of confusion or of misunderstanding." Minn. Stat. § 325.44, subds. 1(5) and (13).

186. By the acts and conduct alleged herein, Defendants committed unfair or deceptive acts and practices by:

a. failing to maintain adequate computer systems and data security practices to safeguard Private Information;

b. failing to disclose that their computer systems and data security practices were inadequate to safeguard Private Information from theft;

c. continued gathering and storage of Private Information after Defendants knew or should have known of the security vulnerabilities of their computer systems that were exploited in the Data Breach;

d. making and using false promises, including, but not limited to, those set out in the Privacy Notice, about the privacy and security of the Private Information of Plaintiff and Class Members, and;

e. continued gathering and storage of Private Information after Defendants knew or should have known of the Data Breach and before Defendants allegedly remediated the data security incident.

187. These unfair acts and practices violated duties imposed by laws, including but not limited to the Federal Trade Commission Act, the Gramm- Leach-Bliley Act, and Minn. Stat. § 325.44.

188. The foregoing deceptive acts and practices were directed at consumers/purchasers.

189. Defendants acted "in the course of business, vocation, or occupation" within the meaning of Minn. Stat. § 325.44 when they committed the aforementioned acts and practices.

190. Defendants engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the furnishing of financial services to consumers, including Plaintiff and Class Members.

191. Defendants' acts, practices, and omissions were done in the course of Defendants' business of marketing and furnishing financial services to consumers while in the State of Minnesota.

192. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the financial services provided,

specifically as to the safety and security of Private Information, to induce Plaintiff and Class Members to purchase the same.

193. Defendants' unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in this Complaint are material in that they relate to matters which reasonable persons, including Plaintiff and Class Members, would attach importance to in making their purchasing decisions or conducting themselves regarding the purchase of services from Defendant.

194. As a direct and proximate result of Defendants' multiple, separate violations of Minn. Stat. § 325.44, Plaintiff and the Class Members suffered injuries including, but not limited to: (i) actual identity theft; (ii) the substantial and present risk of future identity theft; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vii) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (viii) the diminished value of Defendants' services they received.

195. Also as a direct result of Defendant's violation of the Minnesota Deceptive Trade Practices Act, Plaintiff and the Class Members are entitled to injunctive relief, including, but not limited to, ordering Defendants to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

196. Plaintiff and Class Members were injured because: (a) they would not have purchased financial services from Defendants had they known the true nature and character of Defendants' data security practices; (b) Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of promises that Defendants would keep their information reasonably secure; and (c) Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of the promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

197. On behalf of themselves and other members of the Class, Plaintiff is entitled to recover legal and/or equitable relief, including an order enjoining Defendants' unlawful conduct, costs, and reasonable attorneys' fees pursuant to Minn. Stat. § 325D.45 and any other just and appropriate relief.

SIXTH CLAIM
Violation of the Minnesota Prevention of Consumer Fraud Act
(Minn. Stat. § 325F.68 *et seq.*)
(On behalf of Plaintiff and the Class)

198. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 198 above as if fully set forth herein.

199. The Minnesota Prevention of Consumer Fraud Act makes unlawful "any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby." Minn. Stat. § 325F.69, subd. 1.

200. "Merchandise" is defined to include "services," such as the medical care sought by Plaintiffs and Class Members from Defendants. Minn. Stat. § 325F.68, subd. 2.

201. As discussed above, Defendants' Privacy Notice informed Plaintiff and Class Members that Defendants would protect their Private Information and use reasonable data security and other measures to safeguard it appropriately.

202. Defendants failed to use adequate data security and other measures to appropriately safeguard Plaintiff's and Class Members' Private Information, and the Data Breach was the result.

203. Plaintiff and Class Members have been injured as a result of the Data Breach.

204. This action benefits the public because Defendants are public-facing institutions that provides alternative financial services for members of the low-income

community, and it has collected—and continues to collect—sensitive Personal Information from its consumers, including Plaintiff and Class Members.

205. Through this action, and pursuant to the private attorney general statute, Plaintiff and Class Members seek damages to compensate them for their loss, injunctive relief to put a stop to Defendants' unlawful practices and require it to take reasonable and adequate data security measures, and attorneys' fees and costspursuant to Minn. Stat. § 8.31, subd. 3a.

SEVENTH CLAIM
Declaratory Judgment
(On behalf of Plaintiff and the Class)

206. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 205.

207. Defendants owe duties of care to Plaintiff and Class Members that require Defendants to adequately secure their PII.

208. Defendants still possess Plaintiff's and Class Members' PII.

209. Defendants do not specify in the Notice of Data Breach letters what steps they have taken to prevent a data breach from occurring again.

210. Plaintiff and Class Members are at risk of harm due to the exposure of their PII and Defendants' failure to address the security failings that lead to such exposure.

211. Plaintiff, therefore, seeks a declaration that (1) each of Defendants' existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply

with their explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

d. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiff and Class Members for a period of ten years; and

h. Meaningfully educating Plaintiff and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, request judgment against Defendants and that the Court grant the following:

1. An order certifying the Class as defined herein, and appointing Plaintiff and her counsel to represent the Class;

2. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII belonging to Plaintiff and Class Members;

3. An order requiring Defendants to:

   a. Engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

   b. Engage third-party security auditors and internal personnel to run automated security monitoring;

   c. Audit, test, and train their security personnel regarding any new or modified procedures;

   d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

   e. Conduct regular database scanning and security checks;

   f. Routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

   g. Purchase credit monitoring services for Plaintiff and Class Members for a period of ten years; and

   h. Meaningfully educate Plaintiff and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

4. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiff and all Class Members;

5. An award of compensatory, statutory, and nominal damages in an amount to be determined at trial;

6. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

7. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

8. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands this matter be tried before a jury.

Respectfully Submitted,

CHESTNUT CAMBRONNE PA

Dated: November 29, 2021

s/ Bryan L. Bleichner

Bryan L. Bleichner (MN #0326689)
Jeffrey D. Bores (MN #227699)
Christopher P. Renz (MN #0313415)
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (952) 336-2940
bbleichner@chestnutcambronne.com
jbores@chestnutcambronne.com
crenz@chestnutcambronne.com

David K. Lietz, Esq.*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW Suite 305
Washington, DC 20016

Tel: (202) 429-2290
dlietz@masonllp.com

Gary M. Klinger, Esq.*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (202) 429-2290
gklinger@masonllp.com

Attorneys for Plaintiff and Putative Class

* Pro Hac Vice Application Forthcoming